



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|-------------------------|---------------------|------------------|
| 09/642,625 | 08/18/2000 | Peter A.J. van der Made | 81924.0001 | 8243 |

7590

03/26/2003

W. SCOTT PETTY
KING & SPALDING
191 PEACHTREE STREET
45TH FLOOR
ATLANTA, GA 30303-1763

EXAMINER

KISS, ERIC B

ART UNIT

PAPER NUMBER

2122

DATE MAILED: 03/26/2003

12

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/642,625

Applicant(s)

VAN DER MADE, PETER A.J.

Examiner

Eric B. Kiss

Art Unit

2122

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 August 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 June 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2,4,5,7,8,11 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-17 have been examined.

Specification

2. The use of the trademarks WINDOWS, PENTIUM, WINDOWS98, INTERNET EXPLORER, VISUAL BASIC, and OS/2 has been noted in this application. They should be capitalized wherever they appear and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner that might adversely affect their validity as trademarks.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 3, 5, 9, and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Art Unit: 2122

Claim 3 contains the trademark/trade name VISUAL BASIC. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe a particular development system and, accordingly, the identification/description is indefinite. Appropriate correction is required.

Claim 5 recites a functional negative limitation that relates to the operation of unclaimed features and is not a natural result of previous method steps.

The term "substantially similar to" in claims 9 and 16 is a relative term which renders the claim indefinite. The term "substantially similar to" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The limitation "wherein the first behavior pattern is substantially similar to the second behavior pattern" is rendered indefinite by the recitation of this term.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1, 2, 4, 5, and 10-12 are rejected under 35 U.S.C. 102(b) as being anticipated by Jieh-Sheng Lee, et al., “A Generic Virus Detection Agent on the Internet,” January 1997, Proceedings of the Thirtieth Hawaii International Conference on System Sciences, vol. 4: pp. 210-219 (hereinafter *Lee et al.*).

As per claim 1, *Lee et al.* disclose a method for identifying presence of malicious code in program code within a computer system, the method comprising: initializing a virtual machine within the computer system, the virtual machine comprising software simulating functionality of a central processing unit and memory (see the first paragraph of section III.C); virtually executing a target program within the virtual machine so that the target program interacts with the computer system only through the virtual machine (emulating the instructions of the target file); analyzing behavior of the target program following virtual execution to identify occurrence of malicious code behavior and indicating in a behavior pattern the occurrence of malicious code behavior (see the second paragraph of section III. D); and terminating the virtual machine after the analyzing process, thereby removing from the computer system a copy of the target program that was contained within the virtual machine (notifying the user of a successful virus detection

and sending a stop signal back to the emulator; see the last two sentences of the second paragraph of section III. D).

As per claim 2, *Lee et al.* further disclose the virtual machine simulating functionality of input/output ports, operating system data areas, and an operating system application program interface (see sections III. C and III. E).

As per claim 4, *Lee et al.* further disclose virtual execution of the target program causing the target program to interact with the simulated operating system application program interface (see sections III. C and III. E).

As per claim 5, *Lee et al.* further disclose the target program being newly introduced to the computer system and not executed prior to virtually executing the target program (the *Lee et al.* method is proposed as an alternative to executing a potential virus on the system, as is typical in conventional trap tools; see paragraph 4 of section III. A).

As per claim 10, *Lee et al.* further disclose the behavior pattern identifying functions executed in the virtual execution of the target program, the method further comprising tracking an order in which the functions are virtually executed by the target program within the virtual machine (see the second paragraph of section III. D).

As per claim 11, *Lee et al.* disclose a method for identifying presence of malicious code in program code within a computer system, the method comprising: initializing a virtual machine within the computer system, the virtual machine comprising software simulating functionality of a central processing unit, memory, and an operating system including interrupt calls to the virtual operating system (see the first paragraph of section III. C); virtually executing a target program within the virtual machine so that the target program interacts with the virtual operating system

Art Unit: 2122

and the virtual central processing unit through the virtual machine (emulating the instructions of the target file); monitoring behavior of the target program following virtual execution to identify presence of malicious code and indicating in a behavior pattern the occurrence of malicious code behavior (see the second paragraph of section III. D); and terminating the virtual machine, leaving behind a record of the behavior pattern characteristic of the analyzed target program (notifying the user of a successful virus detection and sending a stop signal back to the emulator; see the last two sentences of the second paragraph of section III. D).

As per claim 12, *Lee et al.* further disclose the record being in a behavior register in the computer system (see section III. E).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Lee et al.* as applied to claim 1 above, and further in view of "Softworks Limited VBVM Whitepaper," November 1998 (hereinafter *Softworks*).

As per claim 3, *Lee et al.* disclose such a method, including a virtual machine (see disclosure applied above to claim 1) but fail to expressly disclose the virtual machine further

Art Unit: 2122

including a virtual VISUAL BASIC engine. However, *Softworks* teaches a virtual machine containing a virtual VISUAL BASIC engine ("Softworks VBVM" see the first paragraph). Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to modify the method of *Lee et al.* to include a virtual VISUAL BASIC engine as per the teachings of *Softworks*. One would be motivated to do so to gain the advantage of being able to execute/emulate VISUAL BASIC code in a virtual machine environment.

9. Claims 6-9 and 13-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Lee et al.* as applied to claims 1 and 11 above, and further in view of U.S. Patent No. 5,822,517 to Dotan.

As per claims 6 and 9, *Lee et al.* disclose such a method, including analyzing a program by executing the program in a virtual machine to determine a behavior pattern (see disclosure applied above to claim 1), but fail to expressly disclose determining that a first program is modified; analyzing the modified first program to provide a second behavior pattern; and comparing the first behavior pattern to the second behavior pattern. However, Dotan teaches determining that a first program is modified (see column 7, lines 20-35); analyzing the modified first program to provide a second behavior pattern (marking and storing the final state; see column 7, lines 11-19); and comparing the first behavior pattern to the second behavior pattern (see column 7, lines 20-27). Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to modify the method of *Lee et al.* to include determining that a program has been modified and comparing a first behavior pattern to a

Art Unit: 2122

second behavior pattern from a modified version of the first program as per the teachings of Dotan. One would be motivated to do so to enhance virus detection capabilities by detecting programs that are potentially modified by viruses.

As per claim 7, *Lee et al.* further fail to expressly disclose a new behavior pattern being generated each time the first program is modified. However, Dotan further teaches a new behavior pattern (final state data) being generated after each execution, thereby inherently resulting in a new (different) behavior pattern being generated each time the program is modified (see column 6, line 65 through column 7, line 19). Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to further modify the method of *Lee et al.* to include a new behavior pattern being generated each time the program is modified as per the teachings of Dotan. One would be motivated to do so to be able to dynamically detect program modifications.

As per claim 8, *Lee et al.* further fail to expressly disclose introduction of malignant code during modification of the first program being detected by comparing the first behavior pattern to the second behavior pattern. However, Dotan further teaches such a detection of the introduction of malignant code (see column 7, lines 20-36). Therefore, it would have been obvious to one having ordinary skill in the computer art at the time the invention was made to further modify the method of *Lee et al.* to include detection of the introduction of malignant code by behavior pattern comparison as per the teachings of Dotan. One would be motivated to do so to enhance virus detection capabilities by detecting programs that are potentially modified by viruses.

As per claims 13-17, see the disclosure and/or teachings applied above to claims 6-10, respectively. For reasons stated above, such claims also would have been obvious.

Art Unit: 2122

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eric B. Kiss whose telephone number is (703) 305-7737. The examiner can normally be reached on Tue. - Fri., 7:30 am - 5:00 pm. The examiner can also be reached on alternate Mondays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 308-4789.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

(703) 746-7239 (for formal communications intended for entry)

Or:

(703) 746-7240 (for informal or draft communications, please label
"PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

EBK / ~~EBK~~
March 20, 2003


AVIL KHATRI
PRIMARY EXAMINER